CLAIMS

1. Method for secure wireless transmission of information from a sender to a receiver, comprising

obtaining a message and a receiver identity in a sending device;

encrypting the message to be transmitted;

obtaining a transmission channel from the sending device to a receiving device;

obtaining a receiving address from a secure note, in which a pattern is connected to a receiving device;

transmitting the encrypted information to the receiving device;

decrypting the information in the receiving device;

presenting the message to the receiver; and

optionally acknowledging the receipt of the message to the sender.

2. Method as claimed in claim 1, wherein said pattern is a portion of an absolute position pattern coding absolute positions, and that at least one position of an absolute position code is connected to at least one receiving address.

3. Method as claimed in claim 2, wherein the receiving address is obtained by transmitting said one position to a database, in which the absolute position code is associated with said one receiving address, and using said receiving address for the transmission.

4. Method as claimed in claim 1, wherein the message is obtained by using an absolute position pattern coding absolute positions.

5. Method as claimed in claim 2, further comprising the step:

encrypting the message in the sending device by a symmetric key and decrypting the message by the receiving device by the same key.

6. Method as claimed in claim 5, wherein the symmetric key has been agreed upon in advance and is stored in the sending device and the receiving device.

7. Method as claimed in claim 5, further comprising the steps:

adding the symmetric key to the message after encryption with the symmetric key,

encrypting at least the symmetric key by a public key of an asymmetric key having a private key and a public key and belonging to the receiver,

decrypting the symmetric key by the private key of the receiver in the receiving device;

using the symmetric key for decrypting the message.

8. Method as claimed in claim 7, further comprising the steps:

encrypting the already encrypted symmetric key in the sending device by a private key of an asymmetric key having a private key and a public key and belonging to the sender,

obtaining the sender public key by the receiving device, such as from the sending device or a separate server;

decrypting the symmetric key by the public key of the sender in the receiving device and by the private key of the receiver.

9. Method as claimed in claim 1, further comprising the step:

identification of the sender to the sending device, and/or identification of the receiver to the receiving device by a verification means, such as PIN-code, optical, sound, vibration, heat, speed, angle, time, pressure, acceleration, absolute coordinate, handwritten signature, voice recognition, fingerprint sensor, or other biometric means.

10. Method as claimed in claim 1, further comprising the step:

obtaining a random seed for generating encryption key by means of the verification means during the identification step.

11. Method as claimed in claim 1, further comprising the step:

obtaining a random seed for generating an encryption key during the step of obtaining the message.

12. Method as claimed in claim 1, further comprising the step:

generating in the sending device a sender private key and sender public key pair using a random seed obtained using a physical parameter of the sender, such as handwritten signature recognition, fingerprint information or movement of the sending device or of the sending device, such as acceleration, speed, time, vibration etc.

13. Method as claimed in claim 12, wherein the sender public key is added to the message unencrypted, as sender identification.

14. Device for secure wireless transmission of information from a sender to a receiver, comprising:

a sending device arranged for obtaining a message and a receiver identity;

encryption means for encrypting the message to be transmitted;

a transmission channel from the sending device to a receiving device for transmitting the encrypted information to the receiving device;

decryption means for decrypting the information in the receiving device;

display means for presenting the message to the receiver, and

a secure note, in which a pattern is connected to a receiving device.

15. Device as claimed in claim 14, wherein said pattern is a portion of an absolute position pattern coding absolute positions, and at least one position of

an absolute position code is connected to at least one receiving address.

16. Device as claimed in claim 15, wherein the receiving address is obtained by transmitting said one position to a database, in which the absolute position code is associated with said one receiving address, and using said receiving address for the transmission.

17. Method as claimed in claim 14, wherein the message is obtained by using an absolute position pattern coding absolute positions.

18. Device as claimed in claim 14, wherein

the encryption means is arranged to encrypt the message in the sending device by a symmetric key and that the decryption means is arranged to decrypt the message in the receiving device by the same key.

19. Device as claimed in claim 18, wherein the symmetric key has been agreed upon in advance and is stored in the sending device and the receiving device.

20. Device as claimed in claim 18, wherein

the symmetric key is added to the message after encryption with the symmetric key;

the encryption means is arranged to encrypt at least the symmetric key by a public key of an asymmetric key having a private key and a public key and belonging to the receiver;

the decryption means is arranged to decrypt the symmetric key by the private key of the receiver in the receiving device; and

the decryption means is arranged to use the symmetric key for decrypting the message.

21. Device as claimed in claim 20, wherein

the encryption means is arranged to encrypt the already encrypted symmetric key in the sending device by a private key of an asymmetric key having a private key and a public key and belonging to the sender,

the receiving device is arranged to obtain the sender public key, such as from the sending device or a separate server; and

the decryption means is arranged to decrypt the symmetric key by the public key of the sender in the receiving device and by the private key of the receiver.

22. Device as claimed in claim 14, further comprising

a verification means for identification of the sender to the sending device, and/or identification of the receiver to the receiving device, said verification means being arranged to use identification measures, such as PIN-code, optical, sound, vibration, heat, speed, angle, time, pressure, acceleration, absolute coordinate, handwritten signature, voice recognition, fingerprint sensor, or other biometric means.

23. Device as claimed in claim 14, further comprising

encryption key generation means for obtaining a random seed for generating encryption key by means of the verification means during the identification step.

24. Device as claimed in claim 14, further comprising:

encryption key generation means for obtaining a random seed for generating an encryption key during the step of obtaining the message.

25. Device as claimed in claim 14, wherein the sending device is arranged to generate a sender private key and sender public key pair, and is arranged to use a random seed obtained using a physical parameter of the sender, such as handwritten signature recognition, fingerprint information, or movement of the sending device or of the sending device, such as acceleration, speed, time, vibration etc.

26. Device as claimed in claim 26, wherein the sender public key is added to the message unencrypted, as sender identification.